Why Cyber War Will Not and Should Not Have Its Grand Strategist

Martin C. Libicki

Cyber war proponents often argue the domain needs its own Billy Mitchell or Giulio Douhet—strategists with great vision who will declare to the world what great power lies therein.[1] To be sure, cyber war has no shortage of advocates. But as Colin Gray recently observed, "When historians in the future seek to identify a classic book or two on cyber power written in the 1990s and 2000s, they will be hard pressed to locate even the shortest of short-listable items. . . . Certainly they are nowhere near deserving (oxymoronic) instant classic status."[2]

But has the failure of cyber war to generate any such ideal necessarily been a bad thing? There is a case to be made that it is too early to expect such a classic. If the Owl of Minerva flies at dusk, in cyberspace the sun is just above the yardarm; the information revolution is hardly a done deal. But such a case is too easy. What if the fundamental features of cyber war were to remain essentially as they are into the indefinite future? Although highly unlikely, this is not so absurd a proposition. The late Roger Molander of RAND would frequently remind me that the questions we wrestled with in the mid 1990s are no less relevant and no better understood today than they were then.

Even assuming that the cyber domain has yet to stop evolving, it is not clear that a classic strategic treatment of cyber war is possible, or, even if it were, it would be particularly beneficial. In explaining why, this article makes three points. First, the salutary effects of such classics are limited. Second, the basic facts of cyberspace, and hence cyber war, do not suggest that it would be nearly as revolutionary as airpower has been, or anything close. Third, more speculatively, if there were a classic on cyber war, it would likely be pernicious.

Martin C. Libicki, PhD, is a visiting professor at the US Naval Academy and a senior management scientist at RAND focusing on the impact of information technology on domestic and national security. Previously, he worked for the National Defense University, the Navy Staff, and the GAO's Energy and Minerals Division. He holds a master's degree and a PhD from the University of California–Berkeley.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Why Cyber War Will Not and Should Not Have Its Grand Strategist	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI),Strategic Studies Quarterly (SSQ),155 N. Twining St., Bldg 693,Maxwell AFB,AL,36112-6026**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**17**	

The Limited Usefulness of Classics

Clausewitz's *On War* was, is, and will continue to be perhaps *the* classic book on warfare, but it would be an exaggeration to argue that it was an "instant classic." It was published posthumously. Its influence spread slowly—within a generation in Germany and not until after 1945 in the United States. Furthermore, it really is not a book that gained its reputation by talking about land warfare as such. True, all of its chapters between the introduction and conclusion are about land *warfare.* But what made it a classic was its treatment of war itself—that is, the role and purpose of military force within the relations among states and the relationship between the goals of war and its reality in battle ("fog and friction").

In the naval domain the name Mahan is clearly front and center. Mahan lauded naval power as essential to the maintenance of a seafaring state, especially one that wanted to maintain a global empire—not an irrelevant consideration circa 1890 when he published *The Influence of Sea Power upon History, 1660–1783* (such historic dates suggest he was not overly impressed by technology fads). His book argued strenuously for large battle fleets, which by their very presence and concentration ("fleet in being") could dissuade other states from trying to assert sea control on their own behalf. He eschewed the *Jeune Ècole* preference for commerce raiding.

Mahan's work was enormously influential inside the United States (an inspiration for Theodore Roosevelt's Great White Fleet), and perhaps even more outside it. Kaiser Wilhelm was particularly enchanted by it, as were, to only a slightly lesser extent, Jackie Fisher and the British Royal Navy. Although the expensive Anglo-German naval rivalry cannot be entirely laid at Mahan's doorstep, his influence was not trivial, and the rivalry over battleship building hardly played a calming role in that bilateral relationship.

As for naval strategy, Mahan's work was not particularly helpful for those who believed in his doctrine. The Kaiser's love for his fleet kept it in port for the two and a half years after the Battle of Jutland, even though Germany might have had a chance—admittedly, with a substantial amount of luck—to break the blockade on it and the Austro-Hungarian Empire. This blockade ultimately accelerated the Central Powers breaking under the stress of war before the Allies did. Meanwhile, the naval action that nearly broke the war the other way was the success of German

U-boat attacks on Britain's supply lines to North America. In retrospect, the more decisive use for naval power in World War I was closer (albeit with submarines, not surface ships) to the commerce-raiding that Mahan disdained 25 years earlier in favor of grand fleet actions. He had argued these fleet actions were the sine qua non of naval power.

All this suggests that the global enthusiasm over Mahan's writing—which *was* an instant classic—was good neither for world peace nor a productive naval strategy. Perhaps these are tough tests for any analyst to pass, but if we are to laud the writing of great strategic formulations these are not unfair evaluations.

Consider now airpower. Three individuals stand out in the development of post–World War I strategic thought: the writer Giulio Douhet and generals Billy Mitchell and Hugh Trenchard. All three argued that air forces would become an increasingly important component of modern militaries and that military strategy should, correspondingly, reflect that fact. In that insight, they were correct.

Douhet went further to emphasize the role of strategic bombardment in not only winning future wars, but also shortening them (in that respect—if World War II was any indication—he was not correct). There is an important distinction to be made between the tactical or operational use of airpower (to aid ground and naval forces) and its strategic use: to break the enemy's will to resist and destroy its ability to arm itself. In theory, air forces can do both operational and strategic missions; in practice, their resources are limited, and funds used for strategic purposes compete for resources used operationally.

This leads to the question: Was World War II's emphasis on the strategic campaign such a good idea? In the first major war in which this proposition could be truly tested, only three countries were capable of mounting a serious strategic bombing campaign—first Germany, then the United Kingdom and the United States. Germany's efforts did not seem to have accomplished much; it did not force the UK out of the war nor make much of a dent in its war production. The US and UK bombing campaigns certainly had effects, but these effects were purchased at great cost—the Eighth Air Force alone suffered more than 50,000 deaths (by comparison, the entire US Pacific campaign cost twice as many lives). The succeeding decades saw considerable controversy over whether such bombing campaigns were worthwhile, with detractors saying they *increased* Germany's will to resist and, only toward the very end,

impaired its ability to produce war materiel. A recent prominent defense of strategic bombing by Richard Overy maintains they were worthwhile,[3] not for what harm they did to the Germans, but for how much Germany spent (mostly wasted) to counter them. Even if true, that is a far cry from Douhet's rationale ("air power will demoralize foes" to "air power will cause foes to overreact in self-defense"). Admittedly, a B-29 loaded with nuclear weapons can have a considerably greater effect than a B-29 loaded with conventional weapons—a victory for airpower, but only for 15 years until missiles were invented to do the job more efficiently and reliably. Furthermore, it took until NATO's campaign in Kosovo before there was a first, albeit even then arguable, validation of Douhet's thesis.

If the strategic implications of airpower were poorly understood by virtue of their being exaggerated, the operational implications of airpower à la Billy Mitchell (and many others at the time, if not so dramatically) were on point. Airpower *would* rise in importance relative to land and sea weapons. At sea, by 1942 the carrier was universally recognized as the replacement for the battleship, although the carrier was under firm naval control. Only a half-century after World War I, success in gaining air control (the 1967 Six-Day War and Operations Desert Storm and Iraqi Freedom) predisposed and foretold success in ground combat (at least over uncluttered terrain).

The basis for Billy Mitchell's optimism was, in retrospect, clear. Every year, aircraft became faster; flew higher, farther and longer; and could carry more weight (weapons but also cargo). Antiaircraft weapons were improving but not so quickly (targeting radar and analog computing helped but only somewhat). Nor were ground or sea-based weaponry getting more impervious to bomb damage all that quickly. Technology was inexorably shifting the dominance of battle to the skies. That being so, every other decision about the conduct of battle would have to factor the shift-in-power relationships from ground and surface to air accordingly.

As noted, nothing boosted airpower as much as the development of atomic weapons, which seemed to have validated Douhet's thesis, at least ex post facto. The US Air Force came to absorb almost half of the nation's defense budget in the Eisenhower administration. Clearly, a single weapon capable of knocking out cities was going to have a strategic effect on both war and warfare. So, were there any classics in this new *atomic* field, and what good did they do?

The first place to look was a set of essays by Bernard Brodie for the book, *The Absolute Weapon: Atomic Power and World Order*,[4] wherein can be found his famous quote: "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose." His essays do mention deterrence, but the thrust of his writing was not about how to use atomic forces but to drive home the point that a country under serious atomic attack (that is, thousands of atomic bombs) would be effectively destroyed regardless of how well defended it was. Indeed, his essay spends more time on how to lay out cities to maximize their survivability in an atomic war than it does contemplating what a strategy of deterrence might mean for the construction and the use of forces. So, instant classic quote but no instant classic work.

More works followed in the 1950s by Albert Wohlstetter (on the importance of a second-strike capability),[5] Tom Schelling (on strategies that "left something to chance"),[6] and Herman Kahn (on the need for escalation dominance).[7] It was undoubtedly brilliant stuff, but was it necessarily a wise way to fight—or, better yet, avoid—a nuclear war? The classic model of a nuclear confrontation featured ultra-cool decision makers rationally facing the prospect of mega deaths and maneuvering deftly to avoid that and worse. The actual conduct of a nuclear crisis (Cuba 1962) suggested something a little different: world leaders, having stared at the abyss, realized they had come far too close to a nuclear holocaust and never ever wanted to get that close again. Reactions to that near catastrophe included the hotline and the 1963 test ban treaty. Rather than each side making noises as if it would throw the steering wheel out the window (as Schelling's strategy suggested), each instituted measures to ensure and assure others that it had a much better grip. Similarly, strategic thinking, deprived of direct evidence of Soviet thought, tended to assume that the Soviet Union would approach a confrontation much as Americans would—that is, by carefully delineating (if not necessarily observing) a firebreak between conventional and nuclear operations. The opening of the Soviet archives in 1989 indicated that such delineations were not particularly important to them. Fortunately, no one ever had to go to war based on these strategic theories.

Incidentally, none of this infers that such thinkers did not educate the mind by raising key questions. Even when wrong, one cannot help but profit by working through arguments and, in some cases, asking whether

their logic applies to cyberspace. Unfortunately, when such thinkers are cited as authorities—which they inevitably are—their arguments are converted into answers, at least in the minds of their adherents.

The next two domains of conflict—space and spectrum—have no comparably memorable strategic doctrines or assessments associated with them at all. This, alone, should raise the question of why cyberspace should. Once touted as the really high ground, outer space turns out to be merely a nifty place to stick information collection/processing devices—surveillance satellites, communications relays, and timing/navigation systems (e.g., GPS)—and it is not clear that space will always remain competitive vis-à-vis networked unmanned air-breathing systems for the first two roles. Space is not a particularly good place from which to fight wars. It costs a great deal to get something into orbit, and the price per pound has not appreciably fallen since the 1970s. Space-based weapons are not only expensive but, in their current incarnation, take longer to reach their targets than do simple missiles[8]—deorbiting something actually takes some time. Space systems are also quite fragile in the sense that they can be destroyed by a very small object hitting head-on at a relative speed of 36,000 miles an hour, assuming they are both in low-earth orbit. In a contest between a ground-based missile and a satellite, the odds (these days) are on the missile. So, much to the anguish of the space community, here is a domain without a strategic concept, and, at this point, not inappropriately. It is easy, incidentally, to get lost in arcane debates over which orbit in space is truly the high ground that dominates all the other orbits in space (true aficionados wax rhapsodic about controlling the L1 point, which is roughly four times as far from the earth as the moon and sits directly between the sun and the earth).

Finally, a word is needed in defense of the radio-frequency (RF) spectrum as a domain of warfare, mostly because this domain not only lacks a strategic theory but lacks a strong proponent for theory-building. Yet, it is a *physical* domain in which dominance, in the sense that those who can get their signal through and keep others from getting their signal through, thereby gives its possessor a signal advantage in warfare. No serious military power ignores electronic warfare, largely because radio communications allow militaries to coordinate their operations and radar allows detection and tracking of all manner of enemy assets. But the wizards in the business know the purpose of manipulating the use of a spectrum is to enable physical warfare; by itself, electronic warfare is

next to worthless. Similarly, no one seriously thinks that one country can wreak persuasive or dissuasive damage on another by unleashing its electronic warriors on it, although the latter may be the source of some interesting forms of annoyance, particularly if they can interfere with all GPS applications and mobile devices.

The Significance of Warfare in Cyberspace

It should be fairly clear by now that this article will not close with a ringing call for a strategic cyberspace doctrine. As oft noted, such doctrines—even, or especially, if they meet with universal approbation—are as likely to be wrong as they are right.

To start with, cyber warfare and cyber war need to be distinguished from one another. Cyber warfare, like warfare itself, is about the conduct of war, carried out inevitably to further the performance of combat in the physical domain (it can also be considered operational or instrumental cyber war). Cyber war is undertaken to affect the will of the adversary directly (it can also be considered tantamount to strategic cyber war). A similar distinction can be made between electronic warfare and electronic war—the difference being that no one talks about electronic war as something interesting.

First we can ask whether cyber warfare can so alter warfare that warfare—how it is conducted and what one can do with it—needs to be seriously rethought. Although the ultimate answer to that question is empirical and yet to be determined, it is easy to establish that such a question cannot be answered without an important intermediate step. Cyber warfare attacks systems and digital networks. Prior to the 1960s, militaries had no digital networks to attack. A cyber attack carried out against a military today can, at worst, return it to its prenetworked condition (as long as it *has* something to revert to). To argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary. This is a step many proponents of cyber warfare neglect to take.

So how much *does* digital networking improve the workings of a military? First, one does not need digital communications to have RF communications; the latter can be carried out with analog equipment as it was prior to the 1970s, and, to some extent, still is. Second, as helpful as network-centric warfare may have been for the United States, every

other military in the world is less digitized and therefore less susceptible to cyber war than the US military (notwithstanding the possibility that the digital equipment they have is more vulnerable than the equivalent in the hands of US forces).

Thus, the revolutionary impact of cyber warfare can be no greater than the revolutionary impact of digital networking, which is not, itself, a fully tested proposition. The question of how much less entails asking how effective cyber warfare can be at nullifying the advantages of digital networking. The most it can be is 100 percent, but there are many simple measures militaries can take to reduce it well below 100 percent. One is electronic isolation. If a network is disconnected from the rest of the world, it is very difficult for outsiders to penetrate it. In practice, as Buckshot Yankee and Stuxnet proved, it is not enough that a network lacks an Internet address (or a phone number). There also has to be no way for errant bytes to get into these machines via RF links that depend on the strength of the attacker's transmitter. These are challenging problems but hardly insurmountable. For the most part, systems can be immunized against much of cyber warfare if their instructions are difficult to alter without hands-on contact. This could be because the logic is hardwired into the unit, or because the logic can only be replaced by new hardware modules, or the update has to be digitally signed by a known trustworthy source (using reliable cryptographic protocols implemented correctly). This prevents malware or malicious software with rogue instructions from being placed on the machines, which then limits a machine's actions to those prespecified in its programming. Stuxnet, (and its relatives such as Flame) as well as much of cybercrime, and the advanced persistent threat all depend on the possibility of malware (arbitrarily altered instruction sets) to work.[9]

All this suggests that the effect of cyber warfare, if properly recognized, will be far less revolutionary than the putatively revolutionary effect of digitized networking.

In fairness, consider two objections to this argument. One is that militaries cannot revert to their predigitized network state. This may be empirically true, but if true, it says either that (1) such militaries have abjured that option because they *correctly* recognize that the impact of cyber warfare is something they can manage, or (2) the revolutionary impact of cyber warfare is *incorrectly* underappreciated by militaries who consequently digitize without giving sufficient thought to what would

happen if cyber warfare *were* revolutionary. If the former is true, the issue is settled. If the latter is true, then the only way cyber warfare could be revolutionary is if those victimized by it fail to see it was going to be revolutionary. This is the sort of error that is unlikely to be made more than once, if it is even made at all. Consider, by way of example, Stuxnet. If Iranians had understood what Stuxnet *could* have done to them, they would have likely taken pains to ensure that no USB device was accessible. Because it came as a surprise, Stuxnet worked. But can one assign revolutionary strategic impact to a form of warfare that requires it be systematically underestimated before it can work?

The second objection is that while cyber warfare is not much to look at now, it is only to get more important as militaries continue to digitize. This line echoes the argument that aircraft were going to get better every year; thus, what was false today may be true tomorrow. Can the same be said about cyber warfare?

At this point in the article, one distinction between cyber warfare and warfare in all other media must be made: cyber warfare (as well as cyber war) requires that the targets have made mistakes in their implementation and use of digital equipment. In theory, digital machines should only obey their given instructions in service of their owners/operators. In practice, there are variations between what a system actually does and what it is supposed to do that permits cyber warfare to work. But neither the form nor even the existence of these variations is inevitable. They are artifacts of systems programming. Such artifacts can be reduced, perhaps even effectively eradicated. As noted above, even if systems still have errors, users—especially military users—have a great number of steps they can take to reduce vulnerability to cyber warfare. Indeed, many such steps are being taken—and, doubtlessly, more would be taken if the threat from cyber attacks and the like were greater (or at least perceived to be greater) than is currently the case. This is no proof that there will be a declining threat from cyber warfare to advanced militaries (militaries that have failed to advance have little or nothing to attack in cyberspace); it may well grow. The fact that the threat from cyber warfare has to be enabled by the target's decisions weighs against the proposition that cyber warfare can be revolutionary.

Indeed, there is every indication that electronic warfare will continue to generate more consequential effects on the battlefield than cyber warfare because electronic warfare is not an artifact of the other side's poor

decisions. It is an unavoidable aspect of long-distance RF communications. And, as noted, there is no classic strategic treatment of electronic warfare; nor is there indication that such effort is missed.

That leaves the question of whether strategic cyber war can be significant enough to merit some twenty-first-century version of the Douhet proposition: a form of war that can induce countries to stop fighting (or better, avoid starting fights) without having been defeated or threatened on an actual battlefield. Arguments similar to those above can be generated to suggest that such a thesis is not terribly convincing today. Most cyber attacks, once discovered, are resolved and the effects (apart from leaked information) reversed within a period ranging from hours to days. In the long run, even in the highly unlikely event that hackers will always be able to control the systems they attack, the worst that can happen would be to convince people to abandon networking and thus set economies back to where they were in 1995 (when the Internet started to spread beyond universities and defense-related sites).[10] For advanced countries, 1995 is not that much further behind than they are in 2013. Thus an economy subject to continuous, vicious, and expectedly successful attacks would not retrogress as much as a society subject to World War II–level bombing. And cyber attacks have yet to kill anyone. Granted, if societies have evolved in ways that are difficult to reverse, the effects of cyber war on such societies may be worse than if they had never adopted digitized networks in the first place. But such effects, almost by definition, can be used only once—and only if a society's leadership systematically underestimates its vulnerability to cyber war. Of course, if cyber war turns out to be weak, then perhaps they have not underestimated it at all.

Over time, the distance between 1995 and the then-current year will increase, which will, in theory, lend cyber war more leverage than it has today. Perhaps then, it will be possible to write how cyber war has changed everything we know about warfare. Or maybe not. True, just as aircraft grew monotonically more capable from their invention forward, so societies are growing increasingly digitized, with little prospect that they will move backward (unless, cyber attacks prove to be far more powerful and unavoidable than they are today). But the correlation ends there. Aircraft improvement was a contest against a fixed target (the laws of aeronautics, physics, and chemistry); cyber war is a contest against a moving target wherein offense contends with defense. It is not obvious that offense will get continually better, particularly when defense (in the

form of the target's system and software) defines what the offense can do. Granted, hackers are getting better, thanks in part to markets and market-like mechanisms for sharing information about software vulnerabilities. Furthermore, new uses for digitization (e.g., networked cars) are constantly creating new vulnerabilities or new ways for vulnerabilities to do serious damage. But defense is not catatonic. If the problem with cyber attacks gets bad enough, there are more radical steps that can be taken. One example is Apple's iOS operating system, which has successfully resisted malware because it is a fairly closed system (although some countries have been rumored to have prepared and stashed away attacks on it). Another is the consensus reached by security professionals that Java (software) should be disabled on all browsers because it is becoming very difficult for its developer to stay ahead of all the vulnerabilities hackers keep discovering in it. On purely technical grounds, every successive version of Microsoft's products is more malware-resistant than its prior versions. These days operating systems are subverted by insecure applications rather than being attacked directly. So, the technology dynamic that Billy Mitchell employed—even if aircraft cannot do it today, tomorrow's eventually will—does not necessarily translate into cyberspace, even if cyber security may get worse before it gets better.

Then there is the possibility that the strategic effects of cyber war may arise from the interaction of state actors that systematically overestimate its effects (as quasi-apocalyptic statements from both US and Chinese military officials suggest is quite possible). This could lead to unfortunate dynamics, but in the longer run, the problem with such analyses is similar to those analyses that posit leaders to *underestimate* the effects of cyber war and are therefore unprepared in ways that make it more dangerous. Either way, this is an attitude capable of being corrected by events, and, by its very nature, of temporary import (unless one can successfully argue that the *perception* of what cyber attacks *have done* is systematically in error, but that is a hard case to make).

Cyberspace, as it turns out, is ill-suited for grand strategic theories for other reasons. As mentioned earlier, cyberspace *is* changing very quickly in many important respects. Circa 1999, for instance, US cyber war capability, such as it was, housed itself within the US Space Command (disestablished in 2002). In an era in which mischief in cyberspace was most likely perpetrated by individual hackers who were adroit at getting into systems, maneuvering deftly while discovering how they worked,

doing their job, and leaving quietly, its working ethos would have made it a natural fit for something like the US Special Operations Command. Fortunately, that never happened, because within a dozen years, it was clear that hacking was less about individual rough-and-ready hackers and more like a team-based enterprise building malware tools that took commands from afar and otherwise went about their business based on their programmed-in wits. Today, the original fit between cyber war and the space business looks better—although the fit between US Cyber Command and the National Security Agency is quite good itself.

Another difficulty in proposing a grand theory of cyber warfare is that deception lies at the essence of cyber war. Systems, although meant to be under the control of their owners/operators, are tricked into obeying the commands of others. Once the precise nature of the trick is realized, it is relatively straightforward to figure out how to foil that particular attack—requiring hackers to come up with new tricks, which they often but cannot always do. Deception, by nature, introduces its own self-defeating dynamic, because its existence depends on two sides having different notions of what something can do. Success, in certain key respects, is often inherently unpredictable. Those who wrote strategic theory for, say, airpower had the advantage of understanding the interaction between the machine and its aeronautical environment and between weapons and their targets. They could use that solid base to speculate on the relationship between the effects caused by aircraft and the goals for which countries went to war. Those who would write strategic theory for cyberspace have no such foundation. Everything appears contingent, in large part, because it is.

The Possibly Pernicious Effects of Writing a Cyber War Classic

To be fair, it is not easy to counter what some yet-to-be-written cyber war classic would say. Setting forth here the brilliant insights of such a classic would create the tome this article says cannot exist. Yet, if cyber war's forthcoming classic looks like classics in past domains, they are likely to say (1) cyber war is totally important, (2) those who wield its power should fight to win wars on their own rather than helping warriors in other domains, and (3) war fighters in those other domains should take their strategic cues from what takes place in cyberspace.

To say that war in the virtual world can match the horrors of war undergone or contemplated might seem a stretch, but anyone who ventured such an opinion would not stand alone. Joining them would be the US Defense Science Board (which imagined a cyber attack so severe as to merit a nuclear response),[11] some Chinese generals (one of whom casually opined that a cyber attack could be as damaging as a nuclear attack),[12] and even Russian president Vladimir Putin (who said that a cyber war could be worse than conventional warfare—this from the head of a country that lost 25 million in World War II).[13] There is nothing quite like a good nuclear analogy to rally those in favor of an independent cyber-war force. Yet, the mere argument that cyber war is going to be very important hardly says what to do with cyber-war capabilities, apart from keeping them well fed.

Emphasizing the strategic aspects of cyber war over its tactical (alternatively, operational or instrumental) aspects is not necessarily wrong. Because the operational uses of cyber war are neither ethically nor particularly strategically problematic[14]—in that it only substitutes nonlethal for lethal means—there is little reason *not* to use it against military targets. But military targets are generally harder targets than civilian ones. What may produce limited gains on the battlefield may produce huge payoffs off the battlefield, thereby tempting the elevation of the strategic over the operational.[15] But such elevation has consequences. It affects the allocation of resources and manpower. If talented cyber warriors convince themselves that strategic warfare offers a better shot at top command slots, they will migrate accordingly. Perhaps if cyber war *is* that important, there will be enough resources and manpower to go around—although the current difficulties in finding enough cyber-security professionals suggest that their supply is not infinite and only time will tell how elastic. However, there are certain resources where serious choices must be made: that is knowledge of vulnerabilities in software that allows cyber warriors into many of their targets. To the extent military and civilian systems rely on the same software and hardware—as they increasingly do, although there are still major differences—then a vulnerability exploited for disruptive/destructive purposes (rather than espionage) is likely to be a vulnerability that can be used only during a small time window. Its availability for strategic purposes limits its availability for military purposes. Hence, choices, notably between operational and strategic cyber war, must be made. Because systems have to be penetrated

well before they are attacked, such choices may have to be made well before the character of the upcoming conflict is clear.[16]

Consider, too, that both forms of cyber war—the strategic and the operational—compete with cyber espionage when it comes to allocating vulnerabilities to exploit.[17] Those who want to reserve the exploit for cyber espionage can make two strong points. First, since penetration, in and of itself, tends to be deliberately stealthy, the vulnerability can remain hidden longer than it can once a disruptive/destructive attack takes place.[18] Second, the yield from cyber espionage can be immediate, while the yield from getting into a system that might be taken down is contingent on a war starting.

Strategic cyber war is far more problematic than its operational cousin. It raises laws-of-armed-conflict issues that operational cyber warfare does not. Similarly, it is more likely to result in escalation and in ways that make conflict resolution more difficult. By contrast, operational cyber warfare ends when kinetic warfare ends, because there is no longer any advantage in making targets more susceptible to kinetic attack when kinetic attack terminates.

If the galvanizing theory emphasizes doctrines such as preemption, further difficulties await. Although exactly how to preempt a cyber attack remains a mystery, there is very little that can be destroyed, and only a narrow class of attacks can be disrupted by actions taken outside one's network. If the doctrine is attractive enough, people will think they have found a way to do so. Unfortunately, the many ambiguities of who is doing what to whom in cyberspace suggest that understanding who is preparing to do what to whom is even harder to discern. Grave mistakes are possible—particularly if the decision to preempt attacks is delegated from the president, as many have suggested it might be.[19]

Finally, what might be those cues that warriors in today's domains should take from cyberspace according to some yet-to-be-written doctrine? Cyber war is sneaky stuff. It relies on deceiving computers, which, in turn, requires deceiving humans who manage these computers. It usually works a great deal better when it comes without warning. Insofar as its success depends on the discovery of impermanent elements in the target system, laid-in attacks have to be used quickly if they are to be used at all. Furthermore, because many of its effects are temporary, they must be exploited in a very short time (as quickly as within hours and days). In that sense, powerful cyber attacks can pull follow-up strategic or

operational actions behind them, whether or not the latter are, respectively, appropriate or ready. Cyber war is also an elite activity in which numbers of hackers count for little but the skills of the best of the best count for a great deal.

Cyber operations are covered in heavy layers of secrecy. In some ways, secrecy is deserved: vulnerabilities described quickly become vulnerabilities eradicated. But in other cases, it is questionable: no country admitted to having cyber-war forces until 2012. And in other ways, particularly when disclosing information about vulnerabilities that the other side found in the systems of commercial organizations, it can get in the way. All this makes it difficult to have a serious public debate about the role of cyber war in national security. To be fair, the common difficulty of understanding cyberspace also interferes with useful public debate. Hence the question: Would it be beneficial for the mores of physical war fighting to reflect the inherent mores of war fighting in cyberspace? Perhaps not.

Conclusions

So, rather than bemoan the fact that there are no instant strategic classics on cyber war, or even well-percolated ones, perhaps we should count ourselves lucky. Many of the strategic classics from earlier domains seem to have been misleading, even harmful. War fighters that deal with the more recent media, such as outer space or the radio-frequency spectrum, seem to be doing just fine without them. And cyber war appears to have even less basis for a strategic treatment than space warfare or electronic warfare. Its efficacy—much less significance—has been postulated well before it has been proven. By its very nature, cyber war has to continually morph to retain its relevance. Furthermore, there are good reasons to believe that its contribution to warfare, while real, is likely to be modest, while its contribution to strategic war is a great deal easier to imagine than to substantiate. SSQ

Notes

1. To those who think the argument in favor of finding a Billy Mitchell for cyberspace is a straw man, note the following requests from Frank Cilluffo, former special assistant to the president for homeland security: "We must find the cyber equivalents of Billy Mitchell, George Patton, Curtis LeMay and Bill Donovan—leaders who understand both the tactical and strategic uses of new technologies and weapons," http://www.gwumc.edu/hspi/policy

/Cilluffo_Knop.pdf); Stewart Baker, former general counsel of NSA: "As Brig Gen Billy Mitchell predicted, airpower allowed a devastating and unprecedented strike on our ships in Pearl Harbor. We responded with an outpouring of new technologies, new weapons and new strategies. Today the threat of new cyber weapons is just as real, but we have responded with an outpouring—not of technology or strategy but of law review articles, legal opinions and legal restrictions," http://www.steptoe.com/publications-8146.html; Robert Cringeley, an influential columnist in the IT trade press: "My fear is that when it comes to cyber warfare there is no Billy Mitchell today in Washington," http://www.cringely.com/2009/06/01/remember-billy-mitchell/; George Stein writing in *Air Power Journal* in 1995: "In some ways, 'info-warriors' are like Gen William ('Billy') Mitchell and the pioneer league of airmen. They see the potential. Mitchell's vision of the potential for airpower drove, at great cost to himself but great benefit to the nation, the development of a new form of warfare"; and Robert Lee writing in *Air and Space Power Journal* in 2013: "theorists and military officers, including Gen Giulio Douhet, Marshal of the Royal Air Force Hugh Trenchard, and Brig Gen William 'Billy' Mitchell, helped guide the direction of airpower. As cyberspace reaches its full potential as a domain of warfare equal to the traditional domains, we—like those leaders—must vector it properly."

2. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling* (Carlisle, PA: US Army War College Press, April 2013), viii, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=1147.

3. Richard Overy, *Why the Allies Won* (New York: Norton, 1997). Incidentally, his most recent book, *The Bombing War* (New York: Penguin, 2013), is far more critical of the entire air campaign.

4. Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace, and Co., 1946).

5. Albert Wohlstetter, "The Delicate Balance of Terror," *Foreign Affairs* 37, no. 2 (January 1959): 211–34.

6. Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).

7. Herman Kahn, *On Escalation* (Westport, CT: Praeger, 1965).

8. For a good general treatment, see Robert Preston, *Space Weapons, Earth Wars* (Santa Monica, CA: RAND, 2002).

9. This does not eliminate all sources of cyber warfare. A class of attacks known as SQL (structured query language) injection does not require malware to work, but it only works against systems that accept structured queries, which very few weapons systems do.

10. In the short run, it is possible that an errant set of codes can break equipment, as happened to Iran's nuclear centrifuges following Stuxnet. There is considerable disagreement about whether Stuxnet can be replicated. Its revelation, incidentally, by illustrating what is theoretically possible may have made a repeat performance practically much more difficult because systems managers came to understand they expose their sensitive production and control equipment to the outside at their peril.

11. "The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War." Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington: DoD, January 2013), ES-1.

12. "The United States and China held their highest-level military talks in nearly two years on Monday, with a senior Chinese general pledging to work with the United States on cybersecurity because the consequences of a major cyberattack 'may be as serious as a nuclear bomb.'" Jane Perlez, "U.S. and China put Focus on Cybersecurity," *New York Times*, 23 April 2013, www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html.

13. "[Putin] warned that damage from cyberattacks could be higher than that of conventional weapons." "Putin Urges Readiness against Cyber and Outer Space Attacks," *RIA Novosti*, 5 July 2013, www.rianovosti.com/russia/20130705/182079750/Putin-Urges-Readiness-Against-Cyber-and-Outer-Space-Attacks.html.

14. "Particularly" inserted to the extent there are not fully explored stability impacts of using cyber war as the opening shot of a kinetic engagement or using any form of warfare where attribution is less than obvious.

15. In March 2013, "The chief of the military's newly created Cyber Command told Congress . . . that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks." Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate against Cyberattacks," *New York Times*, 12 March 2013, http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html. It would seem, from such comments, that these offensive teams would be oriented toward strategic rather than tactical missions.

16. That NATO actions against Gadhafi were unforeseen months before they took place was a key reason that cyber attacks were not used to take out Libyan air defenses. See Ellen Nakashima, "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses," *Washington Post*, 17 October 2011, http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn.

17. Not every exploit, however, requires a software vulnerability. Some can be penetrated and exploited by poor systems administration, notably but not exclusively, poor password management.

18. A year is roughly the time that a typical (discovered) advanced persistent threat attack lasts prior to its discovery. Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units*, http://intelreport.mandiant.com/. A year is also roughly the time that a discovered vulnerability sold on the vulnerability market remains undiscovered by anyone else. Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *New York Times*, 14 July 2013, www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

19. David Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*, 3 February 2013, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html.